NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

ACCESS RIGHTS MANAGEMENT

Secure Access for the Financial Services Sector

The National Cybersecurity Center of Excellence (NCCoE) is addressing Access Rights Management (ARM) for the financial services sector through collaboration with members of the sector and vendors of cybersecurity solutions. The example solution proposed by this effort will not be the only one available in the fast-moving cybersecurity technology market. Please contact us at financial_nccoe@nist.gov with suggestions and comments.

CHALLENGE

Some of the identity and access systems employed by the financial services sector are fragmented, incompatible, and operate in isolation from one another. Their operation, therefore, is complex and prone to errors and inconsistencies that can be exploited by attackers or insider threats. This situation makes it difficult for enterprises to securely embrace new technologies such as mobile and cloud computing.

The financial services sector needs the ability to centrally issue, validate, and modify or revoke access rights for an entire enterprise based on easy-to-understand business rules. The goal of this use case is to demonstrate ways to link the management of existing disparate identity and access mechanisms and systems into a comprehensive access rights management (ARM) solution.

SOLUTION

ARM is meant to abstract, unify, and simplify the complex task of dealing with multiple types of access systems, such as Windows Active Directory, Unix/Linux, Resource Access Control Facility (RACF), automatic class selection (ACS2), and myriad legacy and internally developed application-specific mechanisms. The capability will also produce consolidated reports and statistics so that administrators and managers can make accurate risk management decisions.

The ARM system proposed here is designed to provide:

- a single system that is capable of interacting with multiple existing access management systems for a complete picture of access rights within the organization
- secure communications between all components
- automated logging, reporting, and alerting of identity and access management events across the enterprise
- ad-hoc reporting to answer management, performance, and security questions
- support for multiple access levels for the ARM system (e.g. administrator, operator, viewer)
- protection from the introduction of new attack vectors into existing systems
- a complement to, rather than replacement of, existing security infrastructure

BENEFITS

A properly implemented and administered ARM system can:

- reduce damage caused by a successful insider threat attack by limiting the amount of data that any one person has access to
- limit opportunity for a successful attack by reducing the available attack surface
- increase the probability that investigations of attacks or anomalous system behavior will reach successful conclusions
- reduce complexity, which leads to:
  - » faster and more accurate access policy modifications
  - » fewer policy violations due to access inconsistencies
- simplify compliance by producing automated reports and documentation

ARM can answer the following questions:

- What systems and data does a user have access to?
  - » provide an audit log of what a user has accessed and when
- Which users have access to a particular system or data asset?
  - » provide an audit log of when the asset was accessed and by whom

The National Cybersecurity Center of Excellence at the National Institute of Standards and Technology addresses businesses' most pressing cybersecurity problems with practical, standards-based solutions using commercially available technologies. The NCCoE collaborates with industry, academic, and government experts to build modular, open, end-to-end reference designs that are broadly applicable and repeatable.

LEARN MORE ABOUT NCCOE
Visit https://nccoe.nist.gov

CONTACT US
nccoe@nist.gov
301-975-0200

EXAMPLE SCENARIOS

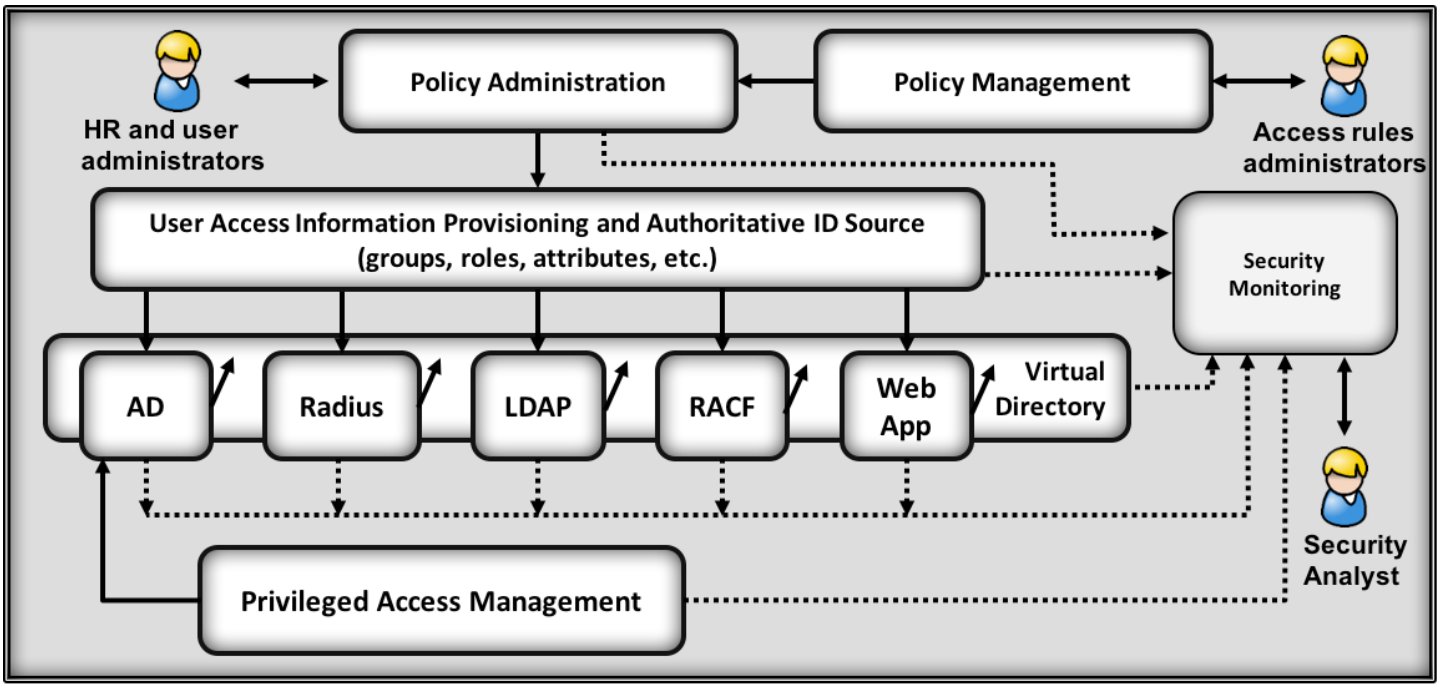
A new employee is hired: ARM uses business rules to develop and implement access rights across the enterprise (e.g., Active Directory, Unix, mainframes) for the new employee.

An employee changes work roles: ARM examines business rules to delete, modify or add access rights across the enterprise that are relevant to the new work role.

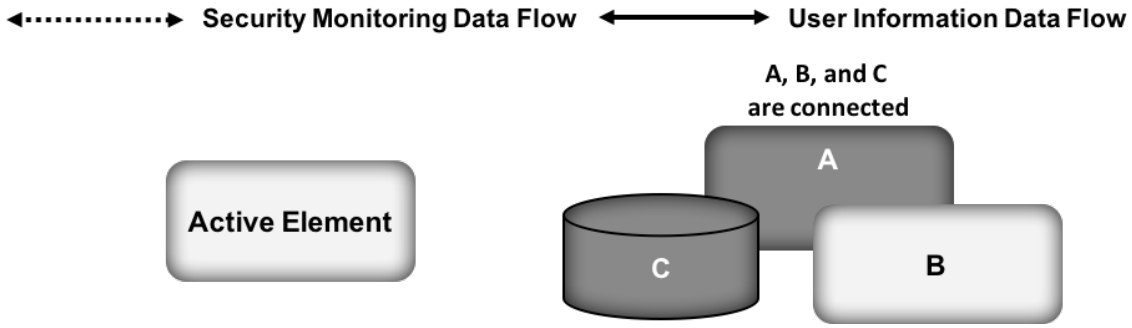
Determine who has access to a particular data asset: ARM ensures that only users with asset rights can access the data asset in question.

HIGH-LEVEL ARCHITECTURE

ARM is a single solution with the ability to interact with existing and future access rights systems by using available communication standards.



Legend



DOWNLOAD THE PRACTICE GUIDE

Visit https://nccoe.nist.gov/projects/use_cases/access_rights_management to learn more about this project.

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking collaborators, insights, and expertise from businesses, the public, and technology vendors. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design, or have questions about applying it in your environment, please contact us at financial_nccoe@nist.gov.

September 2016